

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



IN THE MATTER OF THE SEARCH OF

204 S Holly Avenue
Highland Springs, Virginia 23075

Case No. 3:22-sw-52

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
A WARRANT TO SEARCH AND SEIZE**

I, Daniel Leary, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. The affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I am a Special Agent with the Richmond, Virginia, office of the Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and have been employed as a Special Agent since July 2003. I am currently a member of the Richmond Division Child Exploitation Task Force and have been since March 2018. I have participated in investigations involving sexual assaults, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other

items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2252 and 2252A involving child exploitation offenses.

2. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2252 and 2252A involving child exploitation offenses.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other sworn law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **204 S. Holly Avenue, Highland Springs, Virginia 23075** (hereinafter, the “**SUBJECT PREMISES**”), located within the Eastern District of Virginia and further described in Attachment A, for the things described in Attachment B. Attachments A and B are incorporated herein by reference.

5. I have probable cause to believe that the SUBJECT PREMISES contain contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. §§ 2252A (Receipt, Distribution, and Possession of Child Pornography). I submit this application and affidavit in support of a warrant to search the SUBJECT PREMISES and seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer, communication devices, and electronic media located therein where the items specified in

Attachment B may be found, and to seize all items listed in Attachment B as contraband, instrumentalities, fruits, and evidence of crime.

RELEVANT BACKGROUND INFORMATION AND TERMINOLOGY

I. Characteristics of Collectors of Child Pornography

6. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter, “collectors”).

7. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

8. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

9. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

10. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and

secure location. With the growth of the internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

11. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

12. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

13. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

14. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in that location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

II. Technical Terms

15. Based on my training and experience, I use the following technical terms to

convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **Computer:** As defined pursuant to 18 U.S.C. § 1030(e)(1) is “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and including any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- e. **Computer server or server:** A computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and

delivers information from the server to the user's computer via the internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

- f. **Computer hardware:** Consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but are not limited to, central processing units, internal and peripheral storage devices, such as fixed disks, internal hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but are not limited to, keyboards, printers, video display monitors, and related communication devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but are not limited to, physical keys and locks).
- g. **Computer software:** Digital information which can be interpreted by a computer or any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. **Tablet:** A tablet is a mobile computer that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called applications or "apps," which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- j. **Internet Service Providers (ISPs):** Commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and location of computers and other communication equipment. ISPs can offer a range of options in providing access to the Internet, including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based on the type of connection and volume of data,

called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- k. **Internet Protocol address (or “IP address”):** A unique numeric address used by a computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. Some computers have static, that is long-term IP addresses, while other computers have dynamic, or frequently changed, IP addresses.
- l. **Records, documents and materials:** All information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- m. **Website:** Textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- n. **Storage medium:** Any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, external hard drives, and other magnetic or optical media.
- o. **Log Files:** Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- p. **Peer-to-peer (P2P):** P2P file sharing is a method of communication available to Internet users through the use of special software or applications. The software is designed to allow users to trade digital files through a network that is formed by linking computers together. A significant distinction between P2P networks and traditional computer networks is that P2P machines generally communicate directly with each other, rather than through a relatively low number of centrally-based servers. Because of the decentralized nature of P2P networks, they are commonly used by collectors and traders of child pornography.
- q. **Smartphone:** A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-party software components commonly referred to as “apps.” Smartphones can access the Internet through cellular as well as Wi-Fi (“wireless fidelity”) networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.
- r. **SIM card:** SIM card stands for a “subscriber identity module” or “subscriber identification module,” which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone’s international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.
- s. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains and records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

III. Computers, Electronic Storage, and Forensic Analysis

16. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is digital data stored on a computer's hard drive or other storage media, or on a smartphone's internal memory or SIM card. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage

medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to possess, receive, distribute and/or produce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

19. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

21. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

USE OF PEER-TO-PEER AND BITTORRENT

22. The instant investigation involves a user of “BitTorrent,” which is an Internet-

based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network.

23. P2P file-sharing is a method of communication available to Internet users using special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

24. BitTorrent is one type of P2P file sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a “torrent” file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The

BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

25. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

26. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

27. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be

transferred between computers.

PROBABLE CAUSE

28. In February and March of 2022, agents of HSI, using law enforcement software on the BitTorrent network, identified IP address **96.253.92.196** (the Target IP Address) distributing child pornography via the BitTorrent network. Using law enforcement software, HSI connected with the target computer and downloaded child pornography from the Target IP Address almost daily, indicating the user is constantly attempting to download and upload these files. Using law enforcement software, agents of HSI were able to download multiple complete files from the Target IP Address, as described below. Reviewing these downloads identified the following download activity:

29. On February 24, 2022, law enforcement downloaded 10 complete video files from the user of the Target IP Address that depicted child pornography, child erotica, or related material. Several of the file names began with the acronym “Pedo”, which is a prefix for relating to children or a reference to being a pedophile. Some of the file names began with the acronym “pthc” which stands for pre-teen hard core. The content of the videos included depictions of the sexual abuse of children as young as 2 years old through around 15 years old, and depictions of a child in bondage being forced to commit sexually explicit acts. An example is file name: Pthc – Colombian Girls 12Yo, 14Yo & Man Preteen PedoSex.mpg, which is a 28 minute and 9 second video that is a collection of shorter videos depicting an adult male sexually abusing prepubescent females. The adult male forces the children to conduct sexual acts to include giving and receiving oral sex, vaginal sex, vaginal penetration with fingers and objects, and anal sex. At approximately the 12 minute and 30 second mark, a video segment begins that depicts a prepubescent female approximately 12 years old mostly naked while wearing a black mask and

thigh high white stockings. The child is positioned on her knees next to a bed with her hands bound in front of her using a black rope that is controlled by the adult male like a leash. A black rope is wrapped around the child's neck several times and is connected to the child's ankles that are also bound by the rope. The adult male uses the ropes to force the female child to conduct oral sex on him. The scene then cuts to a depiction of the female child laying on her back bound by the black rope with her knees bent and spread apart to expose her vagina and anus. The adult male then uses his finger and an object to rub and penetrate the female's anus before he conducts oral sex on the child. For the remainder of the video, the man inserts his penis into the female child's anus and touches her vagina.

30. On March 25, 2022, law enforcement downloaded 5 video files from the user of the Target IP Address that depicted child pornography. The content of the videos depicts children from the approximate age of 4 years old to approximately 12 years old engaged in sexual acts with each other and being sexually abused by adults. An example is file name: PTHC Hussyfan NEW chinesse girl about 10 yrbj.fuck.mpg, which is a 32 minute and 28 second video that focuses on an adult male sexually abusing an approximately 10-year-old child. The video depicts the naked child being forced to conduct oral sex on the adult male. The video depicts several scenes where the adult male abuses the child by rubbing his penis on her vagina or having the child conduct oral sex on the adult male. Later in the video, the child is laying on her back and the adult male engages in vaginal sex with the child until he removes his penis and ejaculates onto the child.

31. On March 28, 2022, law enforcement downloaded 3 video files from the user of the Target IP Address that depicted child pornography. An example is file name: Andina 5Yo Incest Slut Child Anal And Face Cum.mpeg, which is a 7 minute and 15 second video of an

approximate 5-year-old female child being abused by an adult male. The female child is wearing a loose-fitting shirt and dressed in white lace gloves, a white headband, a white garter belt with straps connected to white thigh high stockings. The video depicts several scenes of the large adult male sexually abusing the female child by engaging in vaginal sex in several positions. At one point in the video, the adult male is engaged in vaginal sex with the child positioned on top of him. The adult male's penis comes out of the child's vagina and he intentionally forces his penis into the child's anus as the child screams. In the next scene of the video, the child tries to get away from the man, but he pulls her back, and he rubs his semen and penis across her face before forcing his penis into her mouth.

32. On February 18, 2022, I served Verizon with a Summons for subscriber information related to the use of IP address 96.253.92.196, the Target IP Address, on February 14, 2022 through February 18, 2022, which corresponded to dates when child pornography was downloaded from a user of that IP address. A review of the results obtained on March 4, 2022, revealed the following account holder and address, which is the address of the SUBJECT PREMISES: Stella Harding, 204 S Holly Av, Highland Springs, VA 23075.

33. A check of social media, publicly available databases, and law enforcement databases revealed that the residence appears to be occupied by Stella Harding, her husband Spencer Harding, and their son Sean Harding.

34. Intelligence analysis conducted on Sean Harding revealed that he was living in the Tampa, Florida area until about January of 2021, at which time he moved in with his parents at the SUBJECT PREMISES. Prior to his move from Florida, local law enforcement were utilizing software similar to the peer-to-peer software used by HSI in this investigation. Local law enforcement in the Tampa, Florida area had downloaded child pornography from an IP address


subscribed to by Sean Harding. No enforcement action was taken in the local investigation prior to Sean Harding moving from the Tampa, Florida area.

35. On March 14, 2022, HSI Special Agents conducted drive-by surveillance at the SUBJECT PREMISES and observed a white 2014 Hyundai Equus, a white 2012 Ford Explorer and a silver 2014 Hyundai Equus parked in the driveway of the residence. All vehicles are registered to Spencer and/or Stella Harding. The Agents utilized a cellular telephone to connect to local Wi-fi signals as they passed the residence. Many Wi-fi connections were found and all of them were secured with a password.

CONCLUSION

36. Based on the foregoing, I submit that there is probable cause to believe that: (1) an individual or individuals at the SUBJECT PREMISES used a computer or electronic device connected to the internet from the SUBJECT PREMISES to violate Title 18, United States Code §§ 2252 and 2252A; and (2) the fruits, evidence, contraband, and instrumentalities of these offenses, described in Attachment B, are presently located at the SUBJECT PREMISES. Permission is expressly sought to seize any computer hardware, computer software, and computer-related documentation located at the SUBJECT PREMISES and subsequently conduct an on-site and off-site forensic examination, as necessary, using whatever data analysis techniques are needed to seize the contraband, evidence, and instrumentalities listed in Attachment B.

37. I respectfully request, therefore, that the Court issue the attached warrant authorizing the search of the SUBJECT PREMISES described in Attachment A and seizure of the items listed in Attachment B.



Daniel Leary
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN before me on April 5, 2022

/s/ MRC

Mark R. Colombell
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as:
204 S. Holly Avenue
Highland Springs, Virginia 23075

Case No. _____

FILED UNDER SEAL

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is known as

**204 S. Holly Avenue
Highland Springs, Virginia 23075**

The premises is described as a two-story, single-family residence. The house has light green siding and a light grey roof. There is a brick front porch that extends the entire length of the residence with four brick pillars. The front door is in the middle of the residence and is protected by a white storm door. The front door has small glass windows surrounding it along the sides and across the top. There are two regular size windows to the right and left sides of the front door. On the front of the second floor there are 4 windows. The paved driveway is located to the right of the residence. The numbers 204 are posted vertically on the brick front porch pillar immediately to the right of the front steps.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as
204 S. Holly Avenue
Highland Springs, Virginia 23075

Case No. _____

FILED UNDER SEAL

ATTACHMENT B

PROPERTY TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 2252A relating to the distribution, receipt and possession of child pornography, including:
 - a. Any and all visual depictions of minors;
 - b. Any and all address books, names and lists of names and addresses of minors;
 - c. Any and all diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors;
 - d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
 - e. Records and information relating to the BitTorrent network or P2P programs;
 - f. Records and information relating to communications with Internet Protocol (IP) address 96.253.92.196.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. Evidence of who used, owned, or controlled the COMPUTER at the time the things

- described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondences;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. Evidence of the lack of such malicious software;
 - d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.
 - f. Evidence of the times the COMPUTER was used;
 - g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. Records of or information about Internet Protocol addresses used by the COMPUTER;
 - j. Records of, or information about, the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- k. Contextual information necessary to understand the evidence described in this attachment.
- 4. Routers, modems, and network equipment used to connect computers to the Internet.
- 5. During the course of the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.